Genetic Algorithm based Mosaic Image Steganography for Enhanced Security

Soumi C.G[1], Joona George[2], Janahanlal Stephen[3]
[1] Computer Science and Engineering Department, Ilahia College of Engineering and Technology, Kerala, India
[1]Email: cgsoumi@gmail.com
[2, 3] Computer Science and Engineering Department, Ilahia College of Engineering and Technology, Kerala, India
[2]Email:joonageorge@gmail.com
[3]Email: drlalps@gmail.com

Abstract— **The concept of mosaic steganography was proposed by Lai and Tsai [4] for information hiding and retrieval using techniques such as histogram value, greedy search algorithm, and random permutation techniques. In the present paper, a novel method is attempted in mosaic image steganography using techniques such as Genetic algorithm, Key based random permutation .The creation of a predefined database of target images has been avoided. Instead, the randomly selected image is used as the target image reduces the enforced memory load results reduction in the space complexity .GA is used to generate a mapping sequence for tile image hiding. This has resulted in better clarity in the retrieved secret image as well as reduction in computational complexity. The quality of original cover image remains preserved in spite of the embedded data image, thereby better security and robustness is assured. The mosaic image is yielded by dividing the secret image into fragments and embed these tile fragments into the target image based on the mapping sequence by GA and permuted the sequence again by KBRP with a key .The recovery of the secret image is by using the same key and the mapping sequence. This is found to be a lossless data hiding method.**

Index Terms—**GA, MIS, PSNR, mosaics, KBRP, RMSE, Steganography.**

I. Introduction

Steganography is the art of hiding information in other information,. Cryptography is also a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the original message secret. Since in cryptography the encrypted code itself is visible, the concept of steganography has been introduced to embed the message either encrypted or not to make it invisible during communication to secure from eavesdroppers. In other words, Steganography differs from cryptography in the sense that the cryptography focuses on keeping the contents of a message secret whereas the steganography focuses on keeping the existence of a message secret . But, once the presence of hidden information is revealed or sensed oe even suspected, then the purpose of steganography is partly defeated . The strength of steganography can thus be amplified by combining it with cryptography[7].

Existing steganography techniques may be classified into three categories ¯# image, video, and text steganographies [1-3]. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exists a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. Different applications have different requirements of the steganography technique used. For example, some applications may require absolute invisibility of the secret information, while others require a larger secret message to be hidden [6] .In image steganography the information is hidden exclusively in images. The main issue in these techniques is the difficulty to hide a huge amount of image data into the cover image without causing intolerable distortions in the stego-image[5].

Recently, Lai and Tsai [4] proposed a new type of computer art image, called secret-fragment-visible mosaic image, which is the result of random rearrangement of the fragments of a secret image in disguise of another image called target image, creating exactly an effect of image steganography. The above-mentioned difficulty of hiding a huge volume of image data behind a cover image is solved automatically by this type of mosaic image.

Genetic Algorithms (GAs) are search algorithms based on the mechanics of the natural selection process. GAs have the ability to create an initial population of feasible solutions, and then recombine them in a way to guide their search to only the most promising areas of the state space .In mosaic image steganography (MIS) Genetic algorithm is used to generate a mapping sequence by which the tile images are placed on to the target image.

KBRP is a method for generating a particular permutation ***P*** of a given size ***N*** out of ***N!*** Permutations from a given key. This method computes a unique permutation for a specific size since it takes the same key; therefore, the same permutation can be computed each time the same key and size are applied.

Privacy and anonymity is a concern for most people on the internet. Image Steganography allows for two parties to communicate secretly and covertly. It allows for some morally-conscious people to safely whistle blow on internal actions; it allows for copyright protection on digital files using the message as a digital watermark.

One of the other main uses for Image Steganography is for the transportation of high-level or top-secret documents between international governments[13]. While Image

DOI: 01.IJSIP.5.1.17

Steganography has many legitimate uses, it can also be quite nefarious. It can be used by hackers to send viruses and trojans to compromise machines, and also by terrorists and other organizations that rely on covert operations to communicate secretly and safely.

In a visual attack you must have the original "virgin" image to compare it the Steganographed image and visually compare the two for artefacts[13]. In the Enhanced LSB Attack, you process the image for the least significant bits and if the LSB is equal to one, multiply it by 255 so that it becomes its maximum value. Chi-Square Analysis calculates the average LSB and constructs a table of frequencies and Pair of Values; it takes the data from these two tables and performs a chi-square test. It measures the theoretical vs. calculated population difference. The Chi-Square Analysis calculates the chi-square for every 128 bytes of the image. As it iterates through, the chi-square value it calculates becomes more and more accurate until too large of a dataset has been produced.

The remainder of the paper is organized as in the sequence of related works, problem domain, Motivation ,Problem formulation, Proposed methodology of solutions, Simulation, Data model ,Result and Analysis.

II. RELATED WORKS

The original idea of the mosaic image steganography has been proposed by Secret-Fragment-Visible Mosaic Image–A New Computer Art and Its Application to Information Hiding by Lai and Tsai[4].

A new type of art image, called secret-fragment-visible mosaic image[4], which contains small fragments of a given source image is proposed in this study by Lai and Tsai. Observing such a type of mosaic image, one can see all the fragments of the source image, but the fragments are so tiny in size and so random in position that the observer cannot figure out what the source image looks like. Therefore, the source image may be said to be secretly embedded in the resulting mosaic image, though the fragment pieces are all visible to the observer. And this is the reason why the resulting mosaic image is named secret-fragment-visible.

This includes three phases. First is database construction. Second phase is Mosaic image creation and the third is Mosaic image decryption.

The major difficulty of this method is the maintenance of the large database .Because we must calculate the h feature and histogram of each image in the database and also take memory to store these values .Greedy search algorithm is taken more time to find the similarity between the images. So the computational complexity will be very high.

Another study based on mosaic image steganography was done by Li and Wen-Hsiang Tsai by New Image Steganography via Secret-fragment-visible Mosaic Images by Nearly-reversible Color Transformation. Here A new method that creates secret-fragment visible mosaic images with no need of a database [5].Here , any image may be selected as the target image for a given secret image. Figure1 shows a result yielded by this proposed method.

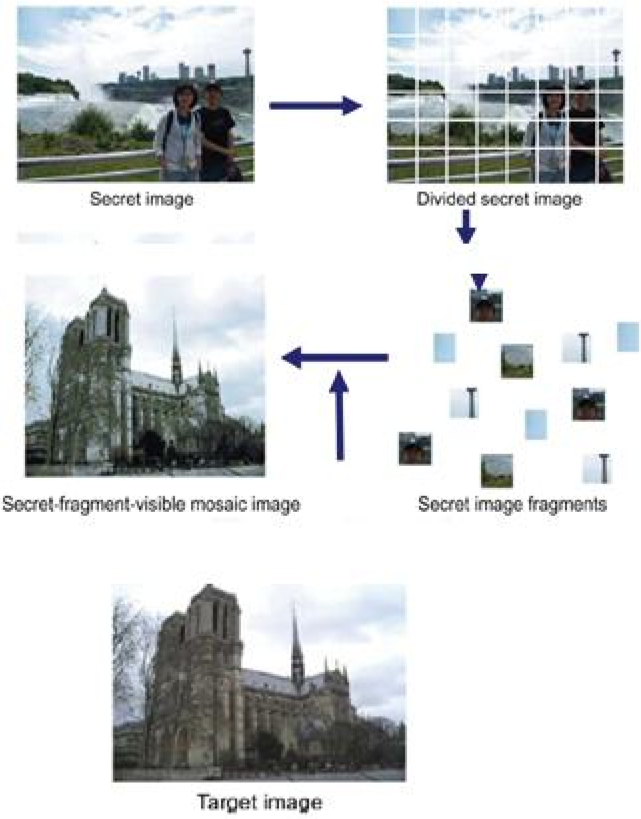


Figure 1. Illustration of creation of secret-fragment-visible mosaic image [4]

A target image is selected arbitrarily, the given secret image is first divided into rectangular fragments, which then are fit into similar blocks in the target image according to a similarity criterion based on color variations. Next, the color characteristic of each tile image is transformed to be that of the corresponding block in the target image, resulting in a mosaic image which looks like the target image. Such a type of camouflage image can be used for securely keeping of a secret image in disguise of any pre-selected target image. Relevant schemes are also proposed to conduct nearly-lossless recovery of the original secret image. Figure 2 shows a result yielded by this method.

The proposed method [5] includes two main phases: mosaic image creation and secret image recovery. The first phase includes four stages:

- fitting the tile images of a given secret image into the target blocks of a pre-selected target image;
- transforming the color characteristic of each tile image in the secret image to become that of the corresponding target block in the target image;
- rotating each tile image into a direction with the minimum RMSE value with respect to its corresponding target block;
- embedding relevant information into the created mosaic image for future recovery of the secret image.

The second phase includes two stages:

- extracting the embedded information for secret image recovery from the mosaic image;
- recover the secret image using the extracted information.

DOI: 01.IJSIP.5.1.17

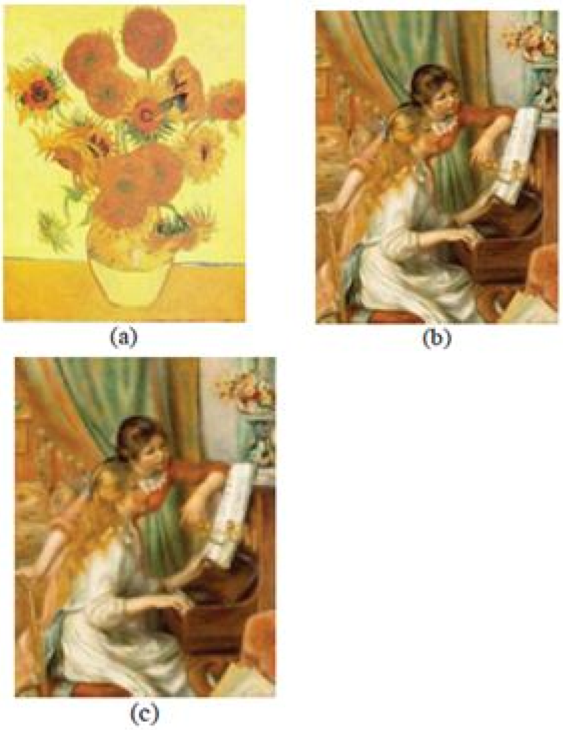


Figure 2. A result yielded by proposed method.(a)Secret image(b) Target image. (c) Secret-fragment-visible mosaic image created from (a) and (b) [5]

The target image can be selected arbitrarily , so to avoid the difficulty of selecting the image from a database. The security is also enhanced compared to former method. Color transformation method is included here for matching purposes.

Here in this paper we present a method for enhanced security and robustness by using Genetic Algorithm.

III. PROBLEM DOMAIN

Images are the most popular cover objects used for steganography. In the domain of digital images many different image file formats exist, most of them for specific applications. For these different image file formats, different steganographic algorithms exist.

To a computer, an image is a collection of numbers that constitute different light intensities in different areas of the image [8]. This numeric representation forms a grid and the individual points are referred to as pixels. Most images on the Internet consists of a rectangular map of the image's pixels (represented as bits) where each pixel is located and its colour [9]. These pixels are displayed horizontally row by row.

The number of bits in a colour scheme, called the bit depth, refers to the number of bits used for each pixel [10].The smallest bit depth in current colour schemes is 8, meaning that there are 8 bits used to describe the colour of each pixel [10]. Monochrome and greyscale images use 8 bits for each pixel and are able to display 256 different colours or shades of grey. Digital colour images are typically stored in 24-bit files and use the RGB colour model, also known as true colour [10]. All colour variations for the pixels of a 24-bit image are derived from three primary colours: red, green and blue, and each primary colour is represented by 8 bits [8]. Thus in one given pixel, there can be 256 different quantities of red, green and blue, adding up to more than 16-million combinations, resulting in more than 16-million colours [10]. Not surprisingly the larger amount of colours that can be displayed, the larger the file size [9].

When working with larger images of greater bit depth, the images tend to become too large to transmit over a standard Internet connection. In order to display an image in a reasonable amount of time, techniques must be incorporated to reduce the image's file size. These techniques make use of mathematical formulae such as for e.g. ,,if we let b and b' denote the number of bits in two representations of the same information , the relative data redundancy R of the representation with b bits is R=(1-1/C) where C , commonly called the compression ratio ,is defined as C=b/b' formula to analyse and condense image data, resulting in smaller file sizes. This process is called compression [9].

In images there are two types of compression: lossy and lossless [11]. Both methods save storage space, but the procedures that they implement differ. Lossy compression creates smaller files by discarding excess image data from the original image. It removes details that are too small for the human eye to differentiate [9], resulting in close approximations of the original image, although not an exact duplicate. An example of an image format that uses this compression technique is JPEG (Joint Photographic Experts Group) [8].

Whereas, Lossless compression, on the other hand, never removes any information from the original image, but instead represents data in mathematical formulas [9]. The original image's integrity is maintained and the decompressed image output is bit-by-bit identical to the original image input [11]. The most popular image formats that use lossless compression is GIF (Graphical Interchange Format) and 8-bit BMP (a Microsoft Windows bitmap file) [8].Compression plays a very important role in choosing which steganographic algorithm to be used. Lossy compression techniques result in smaller image file sizes, but it increases the possibility that the embedded message may be partly lost due to the fact that excess image data will be removed [12].

The advantage of lossless compression is that it keeps the original digital image intact without the chance of loss, although it does not compress the image to such a small file size [8]. Therefore a mosaic image can be saved in a lossless bmp file format for transmission.

In MOSAIC , a given secret image is first "chopped" into tiny rectangular fragments, and a target image with a controlled by a key to fit into the blocks of the target image, yielding a stego-image with a mosaic appearance. The stego-image preserves all the secret image fragments in appearance, but no one can figure out what the original secret image looks like.

However, a large image database is required in order to select a color-similar target image for each input secret image, so that the generated mosaic image can be sufficiently similar

© 2014 ACEEE
DOI: 01.IJSIP.5.1.17

to the selected target image. Using their method, a user is not allowed to select freely his/her favorite image for use as the target image.

The advantage of spatial domain technique used in the project over transform domain of steganography is that the images are first transformed and then the message is embedded in the image [14].Image domain techniques encompass bit-wise methods that apply bit insertion and noise manipulation and are sometimes characterized as "simple systems" [15]. The image formats that are most suitable for image domain steganography are lossless and the techniques are typically dependent on the image format [16]. Steganography in the transform domain involves the manipulation of algorithms and image transforms [15].These methods hide messages in more significant areas of the cover image, making it more robust [17]. Many transform domain methods are independent of the image format and the embedded message may survive conversion between lossy and lossless compression [16].

There are several attacks that one may execute to test for steganographed images that have been subjected to either Visual Attacks or Enhanced LSB Attacks. Chi-Square Analysis, and other statistical analysis methods are employed to identify such hidden information in stegnographed images.

IV. PROBLEM DEFINITION

In the paper by the ref., the authors Lai and Tsai propose a novel method of embedding the secret image in tile form in to the target image in tile form, maintaining the visibility of the original target image selected by greedy search algorithm from the predefined database of target images.

Images are divided into tiles of equal size in matrix form of an image file with the help of MATLAB code. The h feature histogram values of every tiles is extracted and embedded on to the matching tile of target image space, which is a random location in the target image .This is called mosaic information hiding. Based on any random techniques shuffles the tiles again for security. Embedding the tile fitting information in to the blocks of the mosaic image for later recovery.

Sequence of h values e. g Assume a 4x4 matrices of values .Let the cell addresses are : 00 01 02 03 10 11 12 13 20 21 22 23. Let the corresponding h values are: h0 h1 h2 h3 h4 h5 h6 h7 h8h9 h10 h11 ,this is the h value for Pattern 1 . Let the cell address of target: 00 01 02 03 10 11 12 13 20 21 22 23 for target image.Let the corresponding h values are: H11 h5 h8 h6 h0 h1 h4 h9 h10 h2 h3 h7 that is h value pattern 2.Reverse image: h value pattern2 is makes use of to recreate the original secret image.

Whereas in the present work the database of target images is avoided. Any image is selected randomnly as the target image. Both the images are partitioned into tiles by the same concept as in ref.[1].Instead of forming the sequence of h-values, we follow the method of genetic algorithm formed sequence of tiles based on the fitness value .The fitness value is based on the PSNR values of each tile image.

In GA, first create an initial population of n generation of chromosomes (population). Then with the help of PSNR values, and fitness values maximum generations are created by the operations selection and crossover. This leads to the generation of mapping sequence of chromosomes based on the Fitness value. Reverse genetic algorithm is used to decode the mapping sequence.

A new type of art image, called secret-fragment-visible mosaic image, which contains small fragments of a given source image is studied. Observing such a type of mosaic image, one can see all the fragments of the source image, but the fragments are so tiny in size and so random in position that the observer cannot figure out what the source image looks like[4]. Therefore, the source image may be said to be secretly embedded in the resulting mosaic image pieces are all visible to the observer. And this is the reason why the resulting mosaic image is named secret-fragment-visible.

In MIS, the target image is selected from an existing image database which is a pre requirement and enforcing added memory load. Greedy Search algorithm is used for searching the target image from the DB [1]. Searching is based on the h feature and histogram values. This causes higher computational complexity O(n*n logn) for the following reasons. Because searching is progressed on each tiles of a single image for checking h feature values and also for each image in the database for histogram values results this n*n logn complexity.

Using the greedy search algorithm didn't get the optimum result when the target image is small. Greedy algorithm provides optimum results when the image DB is large and the distorted mosaic image results when the DB is small and the proper target image is not selected .Greedy algorithm necessitates a local optimum choice by calculating the h-feature and histogram values o f each image in the DB. Greedy algorithm requires optimum local choices. If locally optimum choices lead to a global optimum and the sub problems are optimal, the greedy works. Greedy algorithm necessitates the local optimums on images. Any DB on image holds for very high storage space and hence leads to high space complexity. Hence it is necessary to search for a method which can reduce the computational complexity an d if possible eliminate the creation of such image DB.

The avoidance of the creation of an image DB necessitates the choice of arbitrarily selecting the target image to hide the secret image in a mosaic form which would call for the generation of mapping sequence **by** genetic algorithm. Once a mapping sequence of tiles is created, enhanced security can be embedded by the selection of security measures such as for e. g: KBRP, chi square analysis or any other random permutation techniques. Using KBRP has the following advantages. computes a unique permutation for a specific size since it takes the same key; therefore, the same permutation can be computed each time the same key and size are applied. the permutation cannot be guessed depending completely on a given key and size. To overcome these disadvantages, this paper proposes another method by using Genetic algorithm . GA resolves the two fundamentally conflicting requirements security and robustness. Here the secret image is divided into tiles and the mapping sequence is generated by using GA.

By using KBRP permuted the sequence again and embedding the tile image fitting information into the first few pixels of the mosaic image. On the retrieving side we can reconstruct the secret image by using the same key and mapping sequence. Another aspect is target image selection which is selected arbitrarily so reduce the memory load.Using this GA can reduce the computational complexity.

Lai, Wen-Hsiang Tsai[5], proposed a method, which creates automatically from an arbitrarily-selected target image a so-called secret fragment-visible mosaic image as a camouflage of a given secret image. The mosaic image is yielded by dividing the secret image into fragments and transforming their color characteristics to be those of the blocks of the target image. Skillful techniques are designed for use in the color transformation process so that the secret image may be recovered nearly lossless. The method not only creates a steganographic effect useful for secure keeping of secret images, but also provides a new way to solve the difficulty of hiding secret images with huge data volumes into target images. The process flow is indicated in the following figure.3.

The block diagram represents the mosaic image creation and recovery. The main important and needful step is the database creation .The accuracy of the image steganography will depends on the selection of the database. Next, select the most accurate image from the database to r match with the secret image. After selecting the most accurate image from the database the next step is to fit the different tile images in to the blocks of the target image keeping both tile images having the same size. The placement of the tile images into the blocks of the target image is based on a key with any random generator sequence .On the retriever side first recover the sequence with the help of the same key and recover the image.

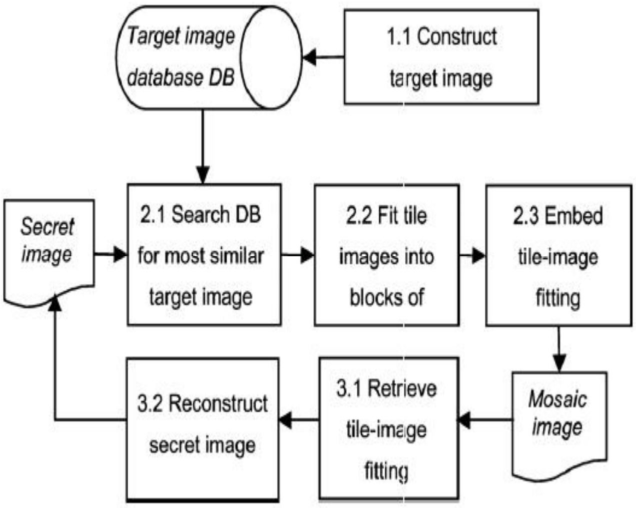

Target image database DB
1.1 Construct target image
Secret image
2.1 Search DB for most similar target image
2.2 Fit tile images into blocks of
2.3 Embed tile-image fitting
Mosaic image
3.1 Retrieve tile-image fitting
3.2 Reconstruct secret image

Figure 3 Processes for secret –fragment-visible mosaic image creation and secret image recovery [4]

V. PROPOSED SYSTEM

The system uses genetic algorithm for gaining additional security and robustness .In addition to this algorithm, we use another algorithm called KBRP. This algorithm helps to generate a random permuted sequence. The permutation is generated from certain key (alphanumeric string) by considering all the elements of this given key in the generation process.

A. *Basic Idea of Proposed Method*

A flow diagram of the proposed method is shown in figure 4, which includes two phases of works.

Phase 1—creation of a secret-fragment-visible mosaic Image using the tile images of a secret image and the arbitrarily selected target image as input;

Phase 2—recovery of the secret image from the created Secret-fragment-visible mosaic image.

The first phase is mosaic image creation. It includes several steps.

- Secret image is divided into several rectangular shaped fragments called tile images of equal size with the target image
- Mapping sequence is generated by GA
- embedding the tile-image fitting information into the mosaic image for later secret image

recovery.

And the Second phase includes two stages of operations:

- retrieving the sequence and the previously-embedded tile-image fitting information from the mosaic image;
- reconstructing the secret image from the mosaic image using the retrieved information.

The concept of MIS by GA can be achieved by hiding the tiles of secret image into the arbitrarily selected target by using GA. The main application of this technique is in confidential areas like military banking sectors etc.

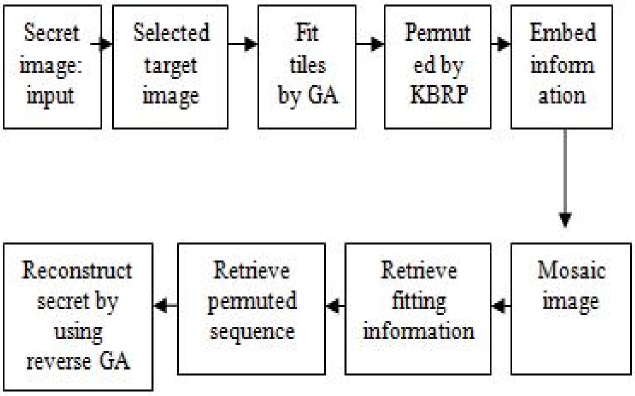


Figure 4 Processes for mosaic image creation and secret image recovery by GA

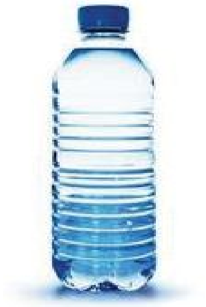
The first step is to divide the secret image into rectangular shaped fragments called tile images of equal size and which are placed into the blocks of the arbitrarily selected target image. The advantage of the proposed system is that the selection of the target image. Any image can be selected as

© 2014 ACEEE
DOI: 01.IJSIP.5.1.17

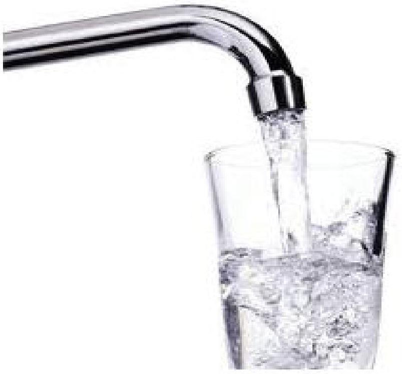
the target image. The target image is also divided into rectangular shaped fragments called tile images of equal size by providing both the target image and the secret image having the same size. We need to hide these tiles of secret in target by creating an efficient mapping function.

The mapping function is generated in several ways . Here, the mapping function is generated by using genetic algorithms (GA). GA is an efficient way to create the mapping sequence than any other methods. Based on this sequence we place the tiles into the target. Next step is to provide additional security by using key based random permutation. It generate a permuted sequence with a key and place the tiles on to the target image for increasing the robustness. The tile image fitting information is embedded on to the first few pixels on the target using LSB embedding scheme and to create the mosaic image.

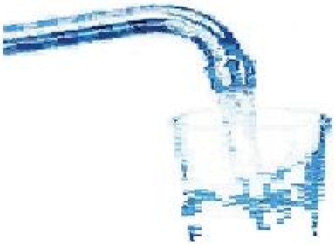
The second Phase is secret image recovery from the created mosaic image by sharing the key. This is by retrieving the embedded information firstly and with the same key we can regenerate the sequence .After this using reverse algorithm we can regenerate the mapping sequence and then the secret image recovery is possible.



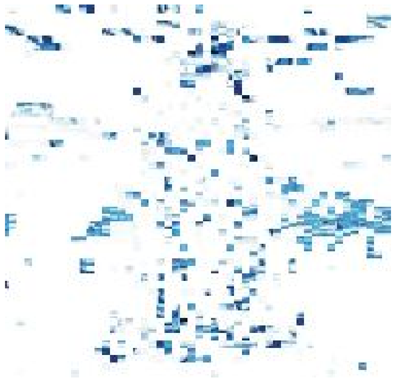
a) Secret image



b)Target image



c) Mosaic image created from a) and b)



d) Noise image with a wrong key

Figure 5 Result yielded by the proposed method. Fig a) represents the secret image Fig b) represents the target image Fig c) represents the created mosaic image from a) and b) and Fig d) represents noise image with a wrong key.

The figure 5 shows the result yielded by the proposed method. Here, Why the retrieved image is blue that the secret image containing white background and the dominant color is blue .Hence that color reflects on the mosaic image.

B) Problem formulation

1. <i/p> Secret image <Process>tile creation-<tool>code in mat lab <o/p> blocks of tiles of size 4x4 matrixes.

2. <i/p>arbitrarily selected Target image <process> tile creation-<tool>code in matlab <o/p>blocks of tiles of size 4x4 matrixes.

3. Fit tiles into blocks of target by GA <i/p>target image and tile blocks <process> GA encryption for sequence generation <o/p>mapping sequence

4. Permuted sequence by KBRP <i/p>key and size <process> generation of unique random permuted sequence <o/p>permuted sequence

5. Embed tile fitting Information <i/p>fitting information like tile size and image size<process> LSB embedding <o/p>mosaic image

6 .Mosaic image

7. Retrieve fitting information <i/p> Mosaic image <process>reverse LSB scheme<o/ p> Mosaic image with permuted sequence

8. Retrieve permuted sequence <i/p>Mosaic image with permuted sequence and key in KBRP<process> using key regenerate random permuted sequence <o/p> permuted sequence

9.Reconstruct secret image by retrieve mapping sequence <i/p> Mosaic image w/o permuted sequence <process>GA decryption <o/p>secret image

VI. Methodology Of Solutions

A) Proposed solutions for Mosaic image creation and recovery

GA used here as an efficient mapping technique for placing the tiles of secret into the target. Genetic Algorithms [18] are the adaptive heuristic search and optimization techniques that mimic the process of natural evolution .This algorithm is an effective stochastic search method, proven as a robust

DOI: 01.IJSIP.5.1.17

problem solving technique that produces better than random results. The algorithm breeds a predetermined number of generations; each generation is populated with a predetermined number of fixed length binary strings. These binary strings are then translated (decoded) into a format that represents suitable parameters either for some controller, or as output. An additional advantage of the genetic algorithm is that the problem solving strategy involves using "the strings' fitness to direct the search; therefore they do not require any problem-specific knowledge of the search space, and they can operate well on search spaces that have gaps, jumps, or noise.

GA operations are based on the population size and the number of generations to be set. If the number of generation in GA increases then the optimum result is achieved but it takes time. The advantage of GA is that it does not break easily even if the inputs varied slightly ,or in the presence of reasonable noise. The algorithm begins with a set of solutions called the initial population. The solutions from one population are taken and used to form a new population. The solutions are selected according to their fitness to form new solutions and this is repeated until some condition is satisfied.

In the proposed system, the first step is to create an initial population. For this determine the values of the population size and the maximum generation size. For each individual generate a random permutation sequence .Then calculate the PSNR values of each block. Based on these determine the Fitness value and select the fittest individuals. Generic operations are performed and replace the population with a new one.

The genetic algorithm optimizes the image quality and security of the data. Each pixel in a block is considered as a chromosome. Some chromosomes are considered for forming an initial population of the first generation in genetic algorithm. Several generations of chromosomes are created to select the best chromosomes by applying the fitness function to replace the original chromosomes. Reproduction randomly duplicates some chromosomes by flipping the second or third lowest bit in the chromosomes. Several second generation chromosomes are generated[19].Crossover is applied by randomly selecting two chromosomes and combining them to generate new chromosomes. This is done to eliminate more duplication in the generations. Mutation changes the bit values in which the data bit is not hidden and exchanges any two genes to generate new chromosome. Once the process of selection, reproduction and mutation is complete, the next block is evaluated. The fitness function enables to optimize the value through several iterations.

To evaluate the expected occurrence (*e*) of a chromosome (*i*) in the mating pool, the fitness of a chromosome (*f*) is divided by the sum of the fitness of all chromosomes in a population [10].*The Probability of Selection.*

$$pselect_i = \frac{f_i}{\sum_{k-1}^{n} f_k} \tag{1}$$

The Expected Occurrence in Mating Pool

$$e_i = pselect_i \times n \tag{2}$$

The flowchart representation of Genetic Algorithm is depicted in figure 6.The first step is to generate an initial population .After setting the population size the next step is the generic operation. Here the crossover and mutation operation is performed. After generic operation is performed the next generation traits is determined. That is, Evaluation step. After evaluation the reproduction stage comes. After ends the reproduction check the exit condition .if the terminal condition arrives stops the algorithm. If the exit condition is not arrived then repeat the steps from generic operation till the condition satisfied.

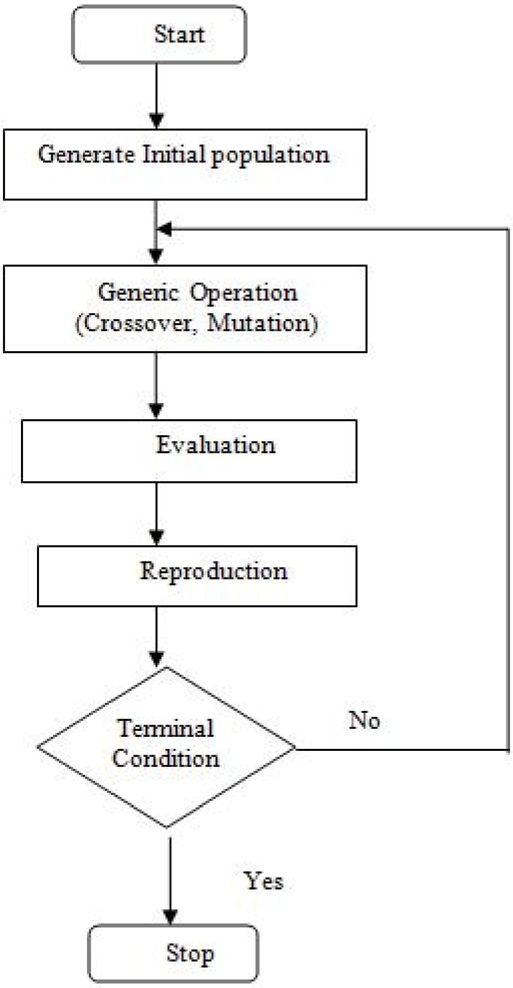

Start
Generate Initial population
Generic Operation (Crossover, Mutation)
Evaluation
Reproduction
Terminal Condition
No
Yes
Stop

Figure 6. Flowchart representation of GA

Another algorithm used in this system is KBRP [20]. The Key Based Random Permutation (KBRP) introduces a method for generating a particular permutation **P** of a given size **N** out of **N!** Permutations from a given key. This method computes a unique permutation for a specific size since it takes the same key; therefore, the same permutation can be computed each time the same key and size are applied. The name of random permutation comes from the fact that the probability of getting this permutation is **1** out of **N!** possible permutations. Besides that, the permutation cannot be

© 2014 ACEEE
DOI: 01.IJSIP.5.1.17

guessed because of its generating method that is depending completely on a given key and size.

The process involves three consecutive steps: init(), eliminate(), and fill(). First step, init(), is to initialize array of size n with elements from the given key, by taking the ASCII code of each element in the key and storing them in the array consecutively. To complete all elements of the array, we add elements to the array by adding two consecutive values of the array until all the elements of the array are set to values. Finally, all values are set to the range 1 to ***N*** by applying the mode operation. The second step, eliminate(), is to get rid of repeated values by replacing them with value of zero and keep only one value out of these repeated values. Last step, fill(), is to replace all zero values with nonzero values in the range 1 to **N** which are not exist in the array. The resulted array now represents the permutation.

VII. Algorithm Of Solutions

ALGORITHM 1: for creating the mapping sequence.

1. [Start] Generate random population of n chromosomes.
2. [Fitness] Evaluate the fitness function f(x) of each Chromosome x in the population.
3. [New Population] create a new population by repeating the following steps until the new population is complete.

    3.1 [Selection] select two parent chromosomes from a Population according to their fitness.

    3.2 [Crossover] with a crossover probability, crossover the parents to form a new offspring. If no crossover i s Performed offspring's is the exact copy of the parents.

    3.3 [Mutation] With a mutation probability, mutate n e w Offspring at each locus.

    3.4 [Accepting] Place new offspring in the new Population
4. [Replace] Use new generated population for a further run of the algorithm.

5 [Test] If the end condition is satisfied, stop, and return the best solution in current population

6. [Loop] Go to step2

ALGORITHM 2 KBRP: for permuting the sequence.

Step1: init()

Initialization step can be shown as follows:

```
Let
K: key (string of alphanumeric) of size S
P: array holds permutation with values 1 to N
N: array size
A[i] = K[i]
for i=1 to S
      P[i] = P[i] + P[i+1]
 for i=1 to S-1
      P[S] = A[1]
While (S < N)
       j = S+1
for( i = 1 to S-1 )
    for( k = i to S-1 && j _ N )
P[i] = P[i] + P[k+1]
j++
P[i] = P[i] MOD N for i = 1 to N
```

Step2: eliminate()

In this step, array **P** contains **N** values. Repetition for some values maybe exists; therefore, the repeated values are examined and replaced with zero. Only one value out of the repeated values is kept in **P**. Now **P** has only distinct values in the range 1 to **N** and some zero values are appeared in **P**. Missing values in the range 1 to **N** that are not exist in **P** will be substituted by the zero elements. This process is shown in the following algorithm:

```
Let
L: left of array P
R: right of array P
For all values where L < R
P[i] = 0 if P[L] = P[i] for i = L+1 to R
P[j] = 0 if P[R] = P[j] for j = R-1 to L+1
Increment L by 1
Decrement R by 1
```

Step3: fill()

The final step, fill(), is to replace any zero value in P by a value in the range 1 to **N** which is not exist in **P**. All zero values will be replaced through a sequence of one value from the left side of P and one value from the right side of P and repeating this sequence until all zero values are gone.This process is shown in the following algorithm:

```
Let
A: array contains missing values in P
m: number of missing values in A
i = 0
while ( i < m )
        j = N

while ( P[i] != 0 && j > 0 )
      decrement j
increment i
k = 1

if ( j > 0 )
        P[j] = A[i]
while ( P[k] != 0 && k _ N )

          increment k
if( k <= N )
     P[k] = A[i]
increment i
```

The resulted array now contains all distinct values in the range 1 to **N** which represents the permutation stored in P.

VIII. Input-Output Model

An input-output model in tabular form is provided in Table 1, where the input data is related to the output data through the processes for easier understanding. The feedback loops are not shown.

TABLE I. INPUT-OUTPUT PROCESS TABLE

Input	Process	Output
Secret image	User input	Accept input image
Target image	Arbitrary selection	Accept as cover image
Blocks of tiles of equal size	Genetic Algorithm	Create a mapping sequence for tile fitting
Hiding image by sequence of tiles in terms of GA	KBRP	Mosaic image
Mosaic image	Provide Key and run KBRP	Hiding image by GA
Image hiding by GA	GA decryption	Secret image

IX. SIMULATION

The proposed methodology is implemented using MATLAB programming. It has mainly two phases. In the encryption phase, first select our secret image and then arbitrarily select our target image.

For encryption, use genetic algorithm and key based random permutation .Using genetic algorithm we can generate an effective mapping sequence and using KBRP the sequence is again permuted. On the decryption phase provided the same key and recover the secret image.

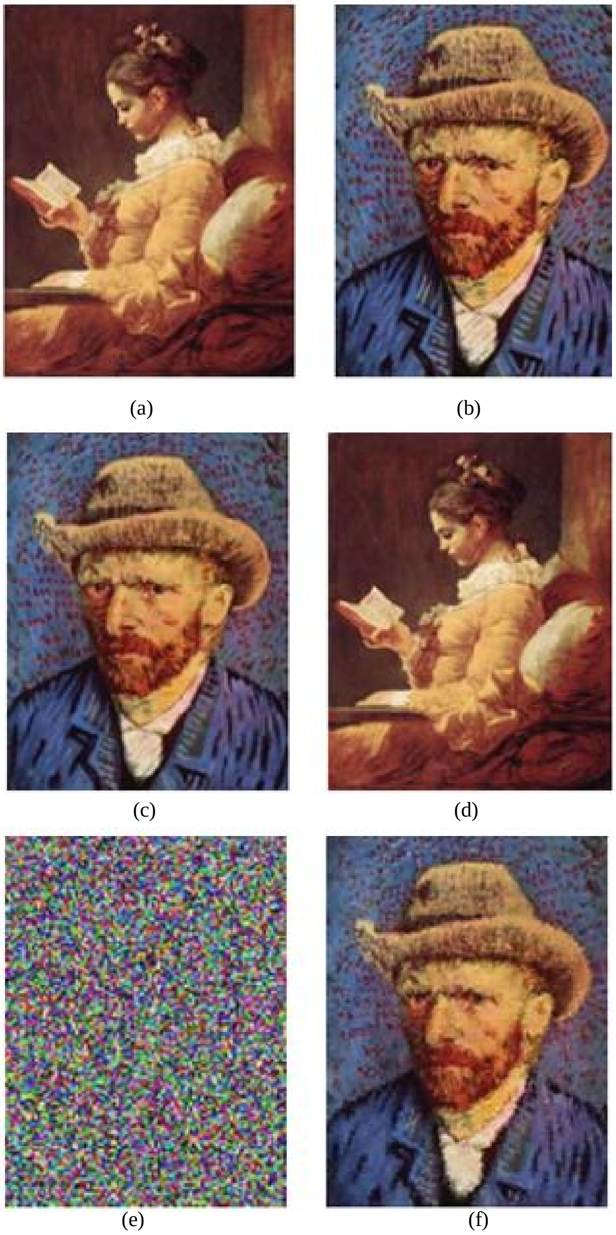
Simulation is done by MATLAB. Here the secret image is effectively hide into the target image by providing both the images having the same size .It is a lossless secret image hiding method.

X. RESULT S

Simulation is done by means of MATLAB. The output is tested with various inputs. A comparative study with different tile image sizes was done and checks the RMSE values of each one.

The result shown in figure.7, where figure 7a) represents a secret image having the size 1024×768 and figure 7b) represents the target image as the same size as the secret image and figure 7c) shows the created mosaic image using figure 7a) and figure7b). Figure 7 d) represents the recovered secret image from the mosaic image with a correct sequence and having PSNR=48.67 and RMSE=0.978 with the secret image. We cannot feel the difference between the two images because PSNR is larger than 30 and RMSE is closer to 1.0.Figure 5 shows that all other results shown have. PSNR values are larger than 47 and RMSE values close to 1.0.

Back to discussions on figure 7) figure 7(e)shows the recovered image having a wrong sequence, which is a noisy image .Figure 7(f),7(g) and7(h) shows different tile images. The analysis of these figures results that the created mosaic image retains more details of the target when the tile image have smaller size (eg:, 4×4 and 8×8).Figure 8 proven this concept. In figure 8a) the tile image size is 8×8 and have smaller RMSE values and when the tile image size is bigger like 32×32 ,the created mosaic image still looks quite similar to the target image. Moreover, the number of bits required for embedding the recovery of secret image is increased when tile image becomes smaller ,is shown in figure 8 b).

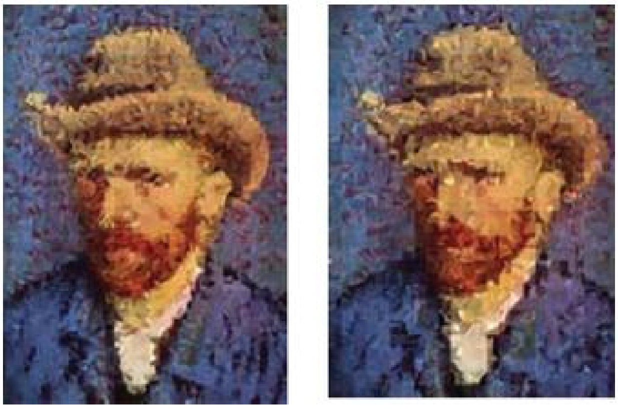


(a) (b)

(c) (d)

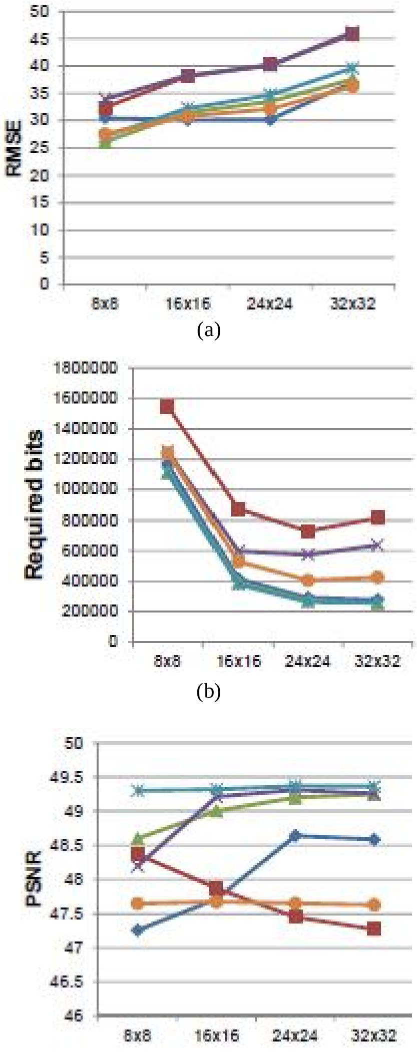
(e) (f)

DOI: 01.IJSIP.5.1.17



(g) (h)

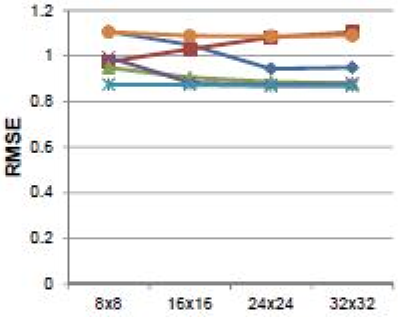
Figure 7 An experimental result of secret-fragment-visible mosaic creation. (a) Secret image. (b) Target image. (c) Mosaic image created with tile image size 8×8. (d) Recovered secret image using a correct sequence with PSNR = 48.67 and with RMSE =0.978 with respect to secret image (a) . (e) Recovered secret image using a wrong sequence. (f)-(h) Mosaic images created with different tile-image sizes 16×16, 24×24, 32×32



(a)

(b)

(c)



(d)

where

— Fig 2
— Fig 5
— Fig 7
— Fig 9a
— Fig 1
— Large dataset

Figure 8 Plots of trends of various parameters versus different tile image sizes (8×8, 16×16,24×24, 32×32) with input secret images all shown previously and a large data set with different secret image and target image pairs. (a) RMSE values of created mosaic images with respect to target images. (b) Numbers of required bits embedded for recovering secret images.(c) PSNR values of recovered secret images with respect to original ones. (d) RMSE values of recovered secret images with respect to original ones

XI. Result Analysis

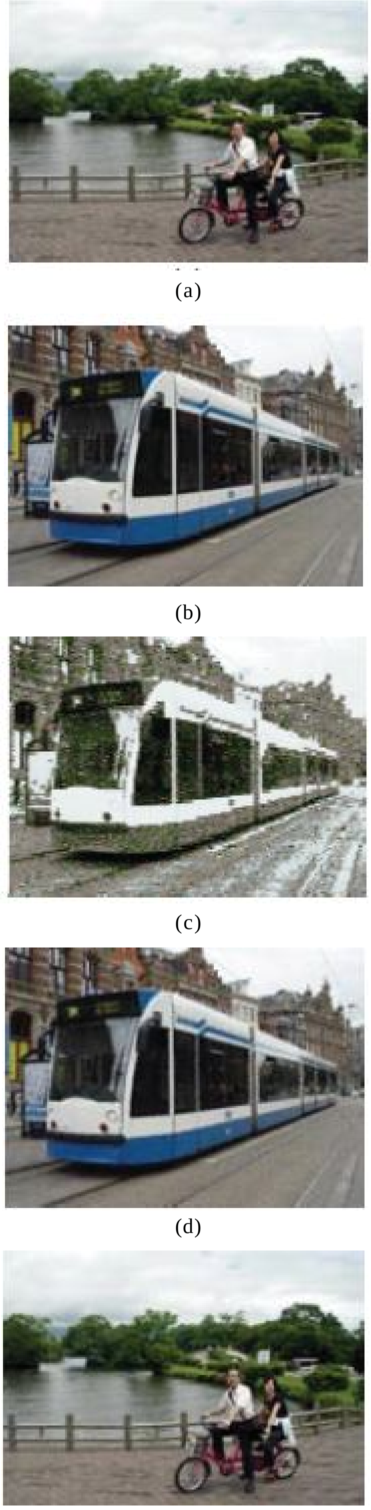
Results with various inputs are checked. The experimental results obtained indicate that the degrees of information hiding is higher using GA, and the different sizes of tile images are selected for verification.

Simulation is done in MATLAB.Different inputs are given. Here, the secret image and target image having the same size and the created mosaic image is based on a mapping sequence by GA and with a key. On the recovery of the secret image, provided the same sequence and key elsewhere the noise image will results.

The peak signal to noise ratio (PSNR) and the RMSE values of the mosaic image is checked and it is above 30 and RMSE is approximately equal to one indicates that the created mosaic image is similar to the target image and the human visual system is difficult to differentiate it. Thus providing the higher degree of information hiding and it should be visually pleasy. Hence it is suitable for covert communication. So it proposed method is a lossless secret image hiding method.

Comparison with the previous method proposed by Lai and Tsai [4] indicates that the proposed method have smaller RMSE values with respect to the target images, indicates that they are more similar to the target images. And noted that, the proposed method allows users to select their favorite images for uses as target images. This provides great flexibility in practical applications without the need to maintain a target image database which usually is very large if mosaic images with high similarities to target images are to be generated. The comparison is shown in figure 9.

DOI: 01.IJSIP.5.1.17



(a)

(b)

(c)

(d)

(e)

Figure 9 Comparison of results of Lai and Tsai [4] and proposed method. (a) Secret image. (b) Target image.(c) Mosaic image created by method proposed by Lai and Tsai [4] with RMSE=47.71. (d) Mosaic image created by proposed method with RMSE =34.10. (e) Recovered secret image with RMSE=0.99 with respect to secret image (a)

XII. Conclusion and Future work

In this paper, a new image steganographic method has been proposed known as Mosaic image steganography based on genetic algorithms for enhanced security. .Its application is not only restricted for covert communication but also handles huge volume of data behind target images. Another important thing is that the target image is selected arbitrarily and hence that no need of a database results saving the memory. Instead of using greedy search , the genetic algorithm reduces the computational complexity in terms of time complexity and space complexity.

The original secret image can be retrieved losselessly from the created mosaic image. The mapping sequence is generated based on genetic algorithm. So the use of genetic algorithm enhances the two fundamentally conflicting requirements security and robustness. The tile image fitting information for secret image recovery is embedded into the first few pixels of the mosaic image by a secret key. The proposed system enhances the visual quality of the image and also focuses on to resist the human visual attack and reducing the statistical attack. The good experimental results shows the feasibility of the proposed method.

As a future work I would like to incorporate the proposed method to images of various color models other than RGB.

Acknowledgement

The authors wish to thank the CSE department for their support and help in completing this work.

References

[1] Bender, W., Gruhl, D., Morimoto, N., Lu, A.: Techniques for Data Hiding. IBM System Journal, Vol 35 ,313-336(1996).

[2] Petit colas, F.A.P., Anderson, R.J., Kuhn, M. G.: Information Hiding - a Survey. Proceedings of IEEE, Vol. 87, No.7,1062-1078 (1999)

[3] Thien, C. C., Lin, J. C.: A Simple and High-hiding Capa,citive method for Hiding Digit-by digit Data in Images Based on Modulus Function, Pattern recognition,.Vol. 36, 28752881 (2003)

[4] Lai, I.J., 3. Tsai, W.H.: Secret-fragment-visible Mosaic Image -A New Computer Art and its application to information hiding, Accepted and to appear in IEEE Transactions on Forensics and Security (2011).

[5] Ya-LinLi1,Wen-Hsiang and Tsai2:New Image Steganography via Secret-fragment-visible Mosaic image by Nearly-reversible Color Transformation unpublished.

[6] Morkel , J.H.P. Eloff , M.S. Olivier “An Overview of Image Steganography,” in Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa June/July 2005.

[7] Wang, H & Wang, S, “Cyber warfare: Steganography,. vs. Steganalysis”, Communications of the ACM,47:10 October 2004.

[8] Johnson, N.F. & Jajodia, S., “Exploring teganography: Seeing the Unseen”, Computer Journal,February, 1998 .

[9] Reference guide:Graphics Technical Optionsand decisions”, 2007, pp. 41-43.

[10] Owenns M., “A discussion of covert channels and steganography” SANS institute,2002

[11] Moerland, T., “Steganography and Steganalysis”, Leiden Institute of Advanced Computing Science,www.liacs.nl/home/

tmoerl/privtech.pdf

[12] Dunbar, B., “Steganographic techniques and their use. in an Open-Systems environment”, SANS Institute January 2002 ,261-289.

[13] Silman, J., “Steganography and Steganalysis: An Overview”, SANS Institute, gsec 1.2f (august 2001)

[14] Lee, Y.K. & Chen, L.H., “High capacity image, steganographic model”, Visual image SignalProcessing, 147:03, June 2000.

[15] Johnson, N.F. & Jajodia, S., “Steganalysis of Images Created Using Current Steganography Proceedings of the 2nd Information Hiding ,April 1998.

[16] Venkatraman, S., Abraham, A. & Paprzycki M “Significance of Steganography on Data Security” Proceedings of the International Conference on Information Technology: Coding and computing, 2004.

[17] Melanie Mitchell :”An introduction to Genetic Algorihtms”, by MIT press, page 1-203,(1998).Author Vitae

[18] Holland, J.H., “Genetic Algorithms,” Scientific American. July 1992, 66-72.

[19] A Genetic Algorithm Tutorial Darrell Whitley Computer Science Department Colorado state university Volume 1, Issue 1, 2010, PP-32-37.

[20] Shakir M. Hussain Journal of Computer Science 2 (5): 419-421, 2006 ISSN 1549-3636© 2006 Science Publications key Based Random Permutation (KBRP) Amman Arab University for Graduate Studies.

BIBILOGRAPHY

Mrs. Soumi C.G completed her B.Tech from Sree Narayana Gurukulam College of Engineering affiliated to M.G University, India in 2008.She did her Post Graduation (M.Tech) in Computer Science and Engineering from Ilahia College of Engineering and Technology under the M.G. University, Kerala, India. Her area of interests are Digital image processing, networks and security.

Mrs. Joona George is an Assistant Professor in the Computer Science and Engineering Department of Ilahia College of Engineering and Technology, Kerala, India. She did her B.Tech in 2009 from Sree Narayana Gurukulam College of Engineering, Kerala, India under the M.G University, followed by her M.E Post Graduation at Vivekanandha College of Engineering for Women, Anna University, Tamilnadu in 2011. Her research areas are Digital Image Processing, Mobile computing and Modern Computer Networks

Professor Dr.Janahanlal Stephen is the Research Dean in the Computer Science and Engineering Department of Ilahia College of Engineering and Technology, Kerala, India. He took his Ph.D from Indian Institute of Technology (IIT),Chennai, India. His research interests are in the area of system dynamic simulation by Prof.J.W.Forrester(formerly of MIT,USA),cloud computing, image processing, and security.